Appendix M— Privacy & Security Framework: Collection, Use, and Disclosure Domain

1 Introduction

The purpose of this document is to provide guidance from the perspective of Nevada's Director of the Department of Health and Human Services (DHHS Director), who is also the designated State Health IT Authority (NRS 439.587), regarding the proper collection, use, and disclosure of patient protected health information (PHI). Establishing a baseline definition for PHI, including specific data elements, stipulating best practices for handling of this data in given situations (de-identification and anonymization of PHI), and specifying requirements for how a patient's PHI can be disclosed based on the required patient consent and in compliance with HIPAA regulations are the goals of this document.

In addition to directing NHIE participants to functionally and procedurally comply with these standards for handling an individual's PHI, the Director also has a number of State specific statutes in place for the Nevada Health Information Exchange. The associated regulations and policies will be detailed and developed by the State within the NHIE governance, technology, procedures, and policies platform by mid 2013.

2 Protected Health Information (PHI)

What is PHI? PHI is individually identifiable health information that is transmitted or maintained in any form or medium - electronic, oral, or paper - by a Covered Entity or its Business Associates, excluding certain educational and employment records. PHI includes any patient information about health status, provision of health care, or payment for health care that can be linked directly to a specific individual's medical record and payment history.

2.1 PHI Ownership

PHI ownership is generally considered to be by the organization from which the PHI originates, for the purposes of handling, transmitting, and sharing the data across a networked environment such as an HIE. However, the actual data content itself belongs to the patient and all handling, disclosure, and consent must comply will HIPAA and any other applicable state and regulations.

2.1.1 The 18 PHI Identifiers

The Health Insurance Portability and Accountability Act defines 18 identifiers which directly links PHI to a specific individual. These identifiers are as follows:

1. Names
2. All geographical identifiers smaller than a state
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax Numbers
6. Email Addresses
7. Social Security Numbers
8. Medical Record Numbers
9. Health Insurance Beneficiary Numbers

10. Account Numbers (of any type)
11. Certificate/License Numbers (of any type)
12. Vehicle identifiers and serial numbers (including license plate numbers)
13. Device identifiers and serial numbers
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers (including finger, retinal and voice prints)
17. Full face (and any comparable) photographic images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

2.1.2 PHI Anonymization

Anonymization is a process whereby all identifiable links and means to an individual are eliminated. Thus, there is no way to identify an individual to any of the health data at hand or the original identifiable data set. This creates unlinkable, totally anonymous data. As the NHIE grows in breadth and depth of its reach of available clinical data, the anonymized study of this data could be an invaluable life science and public health tool for any number of health care research objectives. Thus this ability an understanding of how to anonymize NHIE data will be an important aspect of evolving the NHIE as a population health research (data) resource.

2.1.3 PHI De-Identification

De-identification of PHI may be needed in many circumstances where patient confidentiality/privacy must be maintained with regards to the patients clinical data and outcomes, though a link enabling a a direct and positive tie of an individual to their de-identified clinical data is necessary, for any number of medical, legal, and personal reasons. De-identification of PHI can be accomplished using two methods:

1. Safe Harbor Method - Removal of the 18 common identifiers as listed above.

2. Statistical Method - Obtain the expertise of an experienced statistical expert to validate and document that the statistical risk of re-identification is very small.

2.1.4 Anonymization vs. De-identification - Summary

De-identified data is coded and maintains a link to the original data set of the individual, kept by an honest broker. De-identified data is considered indirectly identifiable and not anonymized. Coded de-identified data is not protected by the HIPAA Privacy Rule, but is protected under the Common Rule. The purpose of the de-identification and anonymization of health data can include research, development, and marketing purposes by universities, government agencies, and private health care entities.

2.2 Data Stewardship

What is Data Stewardship? Data Stewardship (in contrast to data ownership) can be defined as the responsibility of a trusted agent or trading partner – in this example from within the HIE – taking care of PHI/IIHI/EHR or other healthcare data and information which they do not own. And, based on the way data and information is protected under HIPAA, the patient can generally be considered to maintain an ownership over their PHI/IIHI. However, an entity such as a physician or hospital may own an electronic health record (EHR), as the manner in which that EMR is built and maintain is both intellectual and technology property of

the entity and their solutions vendor(s). Within the HIE environment, anyone entrusted with handling this data is a "data steward".

2.2.1 Essential Components of HIE Data Stewardship

Within an HIE, there is a governance element to the oversight of HIE data stewardship. This will be the case within NHIE as well. In order to define accountability and responsibility of the data stewards, there will be essential governance components, or agreements that will maintain the continuity of these relationships and the integrity of the information being traded amongst the NHIE participants. There may be individual or specific instances of PHI/IIHI/EMR data sharing that could require specific agreements between the NHIE and the affected trading prtners, but the essential agreements will include:

Business Associate Agreement (BAA)

- The BAA is the HIPAA agreement for Covered Entities to use when engaging other parties (Business Associates) to perform work for them. This is the fundamental contract the HIE should have with its participants that are HIPAA Covered Entities.

Data Use Agreement

- The Data Use Agreement is used specifically when a limited data set is exchanged with another trusted party for research, public health, or health care operations. This limited data set is individually identifiable health information from which most, but not all, of the 18 HIPAA-specified identifiers have been removed. Although most HIEs, their participants (Covered Entities, Business Associates, etc) will want to exchange PHI/IIHI/EHRs, other uses may be made of a limited data set that would benefit the HIE and other health entities, potentially as a source of revenue.

Data Sharing Agreement

- The Data Sharing Agreement is used between two or more entities within the HIE environment, including the HIE organization itself, who want to share information through the HIE for specifically defined purposes. The Data Sharing Agreement is not defined or required by HIPAA. The agreement can included such specifics as;

    - criteria/purpose for data access,
    - conditions (if any) for certain types of use,
    - specific (or additional to established) privacy, security, and other technical standards with which the data sharing must conform, and
    - whether the data may be de-identified or anonymized (NOTE - when PHI/IIHI is de-identified or anonymized, it is no longer protected under HIPAA. And, although many the HIE and many Covered Entities find it distasteful for organizations with whom they have entrusted their PHI to de-identify/anonymize and sell this data, this may be an important source of revenue for another HIE or trading partner to further its cause of exchange of important information in support of its health care services or its general contributions to the greater HIE).

Participant Agreement

- The Participant Agreement specifies the terms and conditions of the relationship between and responsibilities of each party and commits the HIE and participant to the policies and procedures of the HIE.

2.3 PHI Relative to Public Health

What aspects PHI/IIHI/EMR are impacted by considerations, circumstances, and confidentiality/ privacy rules specific to Public Health? Public health and the local and state level, and as it relates to public health issues reportable up to the federal level present particular challenges that must be met for public health organizations. The HIE can be an advantageous tool in assisting in the efficient and safe exchange of this information. The HIE can help the public health office maintain proper ownership and use monitoring of this information, while providing accurate auditing of the information that is shared and between what organizations. As provisions for PHI relative to Public Health are very specific, the following are excerpts directly from the "Centers for Disease Control and Prevention (CDC) - National Healthcare Safety Network (NHSN) - Provisions Relevant to Public Health Practice" documentation, which addresses major points in this area.

2.3.1 Definition of a Public Health Authority

"*Public health authority* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." (45 CFR Sec 164.501, 65 F. R. p. 82805)

2.3.2 What Information is Protected

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

2.3.3 For What Disclosures and Uses Must Consent Be Obtained

In general, "[a] covered health care provider [with a direct treatment relationship] must obtain the individual's consent,...prior to using or disclosing protected health information to carry out treatment, payment, or health care operations." (45 CFR Sec 164.506, 65 F.R. p. 82810)

2.3.4 Sharing PHI with Public Health Authorities

The Privacy Rule allows for the existing practice of sharing PHI with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. This practice is described in the preamble to the actual Rule:

"The final rule continues to permit covered entities to disclose protected health information without individual authorization directly to public health authorities, such as the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention as well as state and local public health departments, for public health purposes as specified in the NPRM [Notice of Proposed Rulemaking for the Privacy Rule]." (45 CFR 65 F. R. p. 82526)

2.3.5 How Much Information May Be Used, Requested, or Shared

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. (See 45 CFR Sec 164.514(d) for specific requirements.)

> "A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (A) Making disclosures to public officials that are permitted under 45 CFR Sec 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); ..." (See 45 CFR Sec 164.514(d)(3)(iii), 65 F. R. p. 82819)

2.3.6 Who Determines the Minimum PHI for Sharing with Public Health Authorities

Generally, the covered entity is responsible for determining the minimum amount of information reasonably needed to fulfill a request. In certain circumstances, however, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted, for example, when the request is made by a public official or agency for a disclosure permitted under 45 CFR Sec 164.512 of the rule. §164.514(d) of the Rule describes this concept of reasonable reliance:

> "A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (A) Making disclosures to public officials that are permitted under 45 CFR Sec 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); ..." (See 45 CFR Sec 164.514(d)(3)(iii), 65 F. R. p. 82819)

2.3.7 Will the HIPAA Privacy Rule Preserve Existing Strong State Confidentiality Laws

As required by the HIPAA law itself, state laws that provide greater privacy protection (which may be those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

3 Proper and Authorized Use of PHI

3.1 Informed Patient Consent

Why should NHIE proactively encourage Informed Patient Consent? Because informed patient consent;

- promotes a better more interactive, knowledgeable relationship between the patient and their PCP (primary care physician) or other care giver(s), and
- without the very first step of knowledgeable, informed patient consent, there can be no access to, sharing of, and authorized use of the patient's PHI/IIHI/EHR data into the NHIE network as part of the patient's care process.

Informed patient consent is the first essential step to introducing the patient's PHI into the NHIE network. By the patients' understanding of the process and purpose for including their medical data into the NHIE, they are able to make an informed choice to grant or deny permission to allow their PHI to be shared within the NHIE.

The action of *informed* consent is intended to be an open dialogue between the patient and their PCP or other qualified patient care representative who interacts directly with that individual. This affords the patient an opportunity to actively discuss their care situation and process with their doctor or care giver. Thus, the action itself promotes a stronger doctor/patient relationship, a better care experience for the patient, and builds the patient's knowledge and trust base to make the best informed decision regarding the use of their medical information. This use includes providing the individual an understanding of the advantages of sharing their medical information within the NHIE.

Principles of Informed Patient Consent

There are seven key criteria that define informed patient consent;

1. competence to understand and to decide,
2. voluntary decision making,
3. disclosure of material information,
4. recommendation of a plan,
5. comprehension of terms within points 3 and 4,
6. decision in favor of a plan, and
7. authorization of the plan.

A person gives informed consent only if all of these criteria are met. If all of the criteria are met except that the person rejects the plan, that person makes an informed refusal.

Additionally, in the case of a patient granting or denying consent to their care provider to have their medical information shared on the NHIE network, this is a nonemergency situation. In this respect, informed patient consent for NHIE purposes is similar to other nonemergency medical procedures requiring informed patient consent. Written informed consent is generally required before many medical procedures, such as surgery, including biopsies, endoscopy, radiographic procedures, and others. The physician must explain to the patient the diagnosis, the nature of the procedure, including the risks involved and the chances of success, and the alternative methods of treatment that are available. Likewise, for NHIE, the patient's PCP or other care-giver will explain the benefits of HIE to the patient, answer questions, and initiate this process as an ongoing dialogue. But, the goal of this initial NHIE encounter is to obtain the patient's written signature acknowledging the doctor/patient conversation, and explicitly asking the patient's permission (or denial) to share their health information across the NHIE network.

3.2 NHIE Centralized Consent Registry and Management Services

Nevada has taken the position and policy to be an "Opt-In" state (NRS 439.591) for health information exchange and all forms of electronic sharing of PHI/IIHI/EHR data. Medicaid recipients are excluded (NRS. 439.538), and may not opt out of having their IIHI disclosed electronically. As the facilitator of the statewide HIE system, Nevada recognizes that consent management is an important core service that must be provided,

most likely as a registry, tracking, and management function for the ongoing consent preferences of patients throughout the state. The NHIE Centralized Consent Registry and Management Service will satisfy several major requirements, including:

- Provide continuity and uniform patient consent management for each participating HIE and any independent participating stakeholder to the NHIE;
- Eliminate redundancy for both the provider and patient that consent (opt-in) need only be initiated once, but can be accurately managed at the point of any patient encounter with any NHIE participating provider;
- As Nevada is a patient "Opt-In" state for health information exchange and any electronic sharing of PHI/IIHI/EHR data, centralized consent management and registry services will provide:
    - ongoing, on-demand opt-in *and* opt-out of patient participation in the NHIE and electronic data sharing,
    - selective capabilities for a patient to allow or disallow specific aspects of their PHI to be shared,
    - selective capabilities for a patient to allow or restrict PHI sharing with specific NHIE participating providers and stakeholders;
- Establish a level of trust in the NHIE system and services with both the providers and the patients; and
- As a core universal service of NHIE, successful interface to and operating with the NHIE Centralized Consent Registry and Management Service will be a requirement for any HIE or independent provider organization in becoming a Qualified Participant (QP) in the NHIE network.

3.2.1 Establishing Initial Patient Consent (Opt-In or Opt-Out)

It is anticipated that the centralized consent registry and management service will operate in concert with the NHIE master data management (MDM) / enterprise master person index (EMPI) function. This means when the patient presents at an encounter, the patient identity will be validated with NHIE and that patient's consent management record will be made available to the encounter provider. This approach will inform the provider of the patient's selected consent for electronic exchange of their health data.

As an example of central consent management, a potential workflow for initial patient identity and consent management may occur as follows:

- The patient's identity will be confirmed via the NHIE EMPI service;
- If it is determined that the patient is being encountered within the NHIE network for the first time, the centralized consent management process will be invoked to establish that Patient's initial consent record within the NHIE consent registry;
- The provider (or practice office administration) may lead the patient through the proper informed consent process and explicitly describe the NHIE electronic PHI/IIHI/EHR data sharing that will be allowed given preference options;
- The patient may then indicate their desired opt-in or opt-out preference(s), and the central registry would be updated accordingly; and
- Patient will be provided credentials enabling them with the ability to access the centralized consent management function online and to make modifications to their consent preferences (specifics regarding one or two factor credentials will be determined by NHIE in the future).

3.2.2 Managing Patient Consent Preference(s) and Queries

It is anticipated that, at any time after a patient has been established by identity and by consent preference within the NHIE network, the Centralized Patient Consent Registry Service will be able to support full query and editing capability to the patient's consent preferences at any point of encounter with any NHIE participating HIE/provider. The patient's provider may also need to review the patient's consent preferences from time to time in the event of referrals, etc. This will ensure the provider continues to offer the patient informed consent and the opportunity to determine their own consent preferences based on their current medical circumstances.

Utilizing the centralized patient consent management services could include the following functionality:

- Consent Status Queries - Current patient consent status could be queried either from a provider portal, or by a patient if and when NHIE provides patient portal access to the patient consent registry.
- Manage Patient Consent Preference(s) - The provider (as an independent NHIE participant or as part of a participating HIE) on the patient's behalf, or the patient via a patient portal may access the Consent Management Service to change their Opt-In and Opt-Out preference. The patient will have the choice to be selective about provider access preferences, and the type of PHI/IIHI/EHR data that may be shared electronically on the NHIE network.

3.2.3 Transaction Logging and Audit Security

As with any activity and access to patient PHI/IIHI/EHR data, security is a priority of this centralized functionality. Validating all authorized access to the patients consent data, be it by a provider or the patient themselves, and tracing the activity is an important requirement of the security for the NHIE Consent Management and Registry processes. As previously stated, this process will likely work with the NHIE MDM/EMPI functionality for identity management and validation of access to the patient's centralized consent registry – regardless if that access is by an authorized provider or the patient.

As part of maintaining compliant PHI/IIHI/EHR security features, the NHIE Centralized Patient Consent Management process will also track each transaction, the activity performed, the person or entity performing the activity, and the end result of any changes to the patients consent record as a result of a given transaction. These full transaction logs will be maintained by NHIE in accordance with established practices and compliance guidelines for record retention. These records can be requested and available on demand by the patient or appropriate authorized representative or agent as needed. It is likely that additional State statutes will be necessary for Centralized Consent functionality and services, if the state rulemaking process is not sufficient to meet the needs of Nevada residents. Such legislation would then be proposed during the 2015 session of the Nevada Legislature.

4 Senate Bill 34 (SB-43) and Nevada Revised Statutes (NRS) for the Statewide Health Information Exchange System

The Nevada Legislature meets on a biennial basis and is in session for 120 days. Being one of only six US states operating with this type of legislative schedule, Nevada faces unique challenges and constraints in the work it can and must accomplish in this time frame every two years. In the 2011 biennial session, the Nevada Legislature passed Senate Bill 43 (SB-43) and a number of related Nevada Revised Statutes (NRS) specifically

addressing the State's new and evolving HIE – now known as the Nevada Health Information Exchange, or NHIE. Nevada is fully committed to launching, growing, and sustaining NHIE for years to come. SB-43 and NRS 439.581 through NRS 439.595 lay the ground work for beginning the build of the statewide NHIE, and indicating point by point regulatory objectives of the DHHS Director – regulatory objectives which will be further defined and put in place by the next biennial legislative session – and in time for full implementation of the statewide NHIE. In the meantime, Nevada will have a HIE governance and operational body in place. This governance and operational body will begin to build out a statewide HIE by recruiting qualified participant stakeholder organizations from throughout the state, and following the guidelines already set in place by SB-43 and NRS 439.581 through NRS 439.595. Prior to the close of the biennial legislative session in 2015, Nevada's DHHS Director will put additional regulations in place, as indicated, covering the details of all points currently specified in the SB-43 and NRS sections. Along with applicable federal standards and laws, these state requirements will drive the operational compliance and accountability of the NHIE, and state-wide continuity for patient trust and participation will be supported by NHIE centralized services like Consent Management Registry.

5 References & Resources

Supporting reference and resource materials include the following;

1) Health Insurance Portability and Accountability Act (HIPAA), 45 CFR (Privacy Rule/Common Rule)
2) American Health Information Management Association (AHIMA) www.ahima.org See **HIM Principles in Health Information Exchange (Practice Brief)**
   http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035095.hcsp
3) Stratis Health – HIE Data Stewardship
   http://www.stratishealth.org/documents/HITToolkitHH/3.Exchange/3.2Interoperate/3.2HIE_Data_Stewardship.doc
4) Centers for Disease Control and Prevention (CDC) - National Healthcare Safety Network (NHSN)
5) Provisions Relevant to Public Health Practice
   http://www.cdc.gov/nhsn/FAQ_HIPAArules.htm
6) Miller-Keane Encyclopedia and Dictionary of Medicine, Nursing, and Allied Health, Seventh Edition. © 2003
7) *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*, March 23, 2010
   Melissa M. Goldstein, JD, Associate Research Professor, Department of Health Policy, School of Public Health and Health Services, The George Washington University Medical Center, and Alison L. Rein, MS, Director, AcademyHealth